Secure Encoded Instruction Graphs for End-to-End Data Validation in Autonomous Robots

Jorge Peña Queralta[1], Li Qingqing[1], Eduardo Castelló Ferrer[2], Tomi Westerlund[1]

[1]Turku Intelligent Embedded and Robotic Systems, University of Turku, Finland
Email: [1]{jopequ, qingqli, tovewe}@utu.fi

[2]MIT Media Lab, Massachusetts Institute of Technology, USA
Email: [2]ecstll@media.mit.edu

***Abstract*—As autonomous robots become increasingly ubiquitous, more attention is being paid to the security of robotic operation. Autonomous robots can be seen as cyber-physical systems that transverse the virtual realm and operate in the human dimension. As a consequence, securing the operation of autonomous robots goes beyond securing data, from sensor input to mission instructions, towards securing the interaction with their environment. There is a lack of research towards methods that would allow a robot to ensure that both its sensors and actuators are operating correctly without external feedback. This paper introduces a robotic mission encoding method that serves as an end-to-end validation framework for autonomous robots. In particular, we put our framework into practice with a proof of concept describing a novel map encoding method that allows robots to navigate an objective environment with almost-zero a priori knowledge of it, and to validate operational instructions. We also demonstrate the applicability of our framework through experiments with real robots for two different map encoding methods. The encoded maps inherit all the advantages of traditional landmark-based navigation, with the addition of cryptographic hashes that enable end-to-end information validation. This end-to-end validation can be applied to virtually any aspect of robotic operation where there is a predefined set of operations or instructions given to the robot.**

***Index Terms*—Robotics; Autonomous Robots; Robotic Navigation; Cyber-Physical Security; Secure Navigation; Validation in Robotics; Map Encoding;**

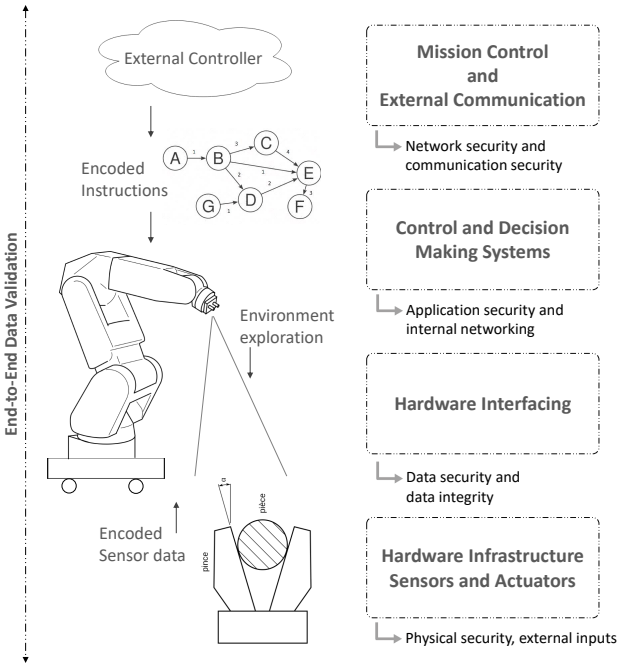

Fig. 1: Classification of data acquisition and analysis processes in autonomous robots and matching security layers.

I. Introduction

With robots and autonomous robots having an increasing penetration across multiple aspects of our society, more attention is being paid to the safety and security aspects in robotic operation [1]. The differentiation between safety and security often becomes fuzzy, with the safety term being utilized to refer to human-robot interaction [2], or to the safety of the robot itself [3]. In either case, safe operation of an autonomous robot requires tight control over the security of the data being used, from data defining mission instructions to sensor data. Figure 1 shows a layered classification of stages in which information is either collected or processed by an autonomous robotic system. This figure extends the cyberattacks categorization in [4], and also takes into consideration that the internal processes can be modeled as a software-defined network from a more abstract point of view [5]. Many robotic frameworks, such as the Robot Operating System (ROS) fall into this consideration [6]. From the cybersecurity domain point of view, the acquired sensor data needs to be secured as well. This represents an additional challenge. Therefore, an essential aspect in the operation of autonomous robots is to be able to validate both data being shared among subsystems and external systems (a controller or other robots), but also data defining or characterizing the way the robot, seen as a cyber-physical system, interacts with its environment.

A relevant precedent in securing multi-robot cooperation was introduced by Castell Ferrer et al. in [7], where the authors leveraged Merkle trees to cope with byzantine robots in cooperative missions within swarms of robots. The main novelty of their work is the introduction of a framework for validating data in robots without relying on the data itself, by encoding mission instructions in Merkle trees. Merkle trees are cryptographic structures that enable validation of data through cryptographic proofs that do not involve the data itself.

We aim at extending previous works into a more general framework focusing on encoding not only of mission instructions but also on the relationship between the possible ways in which a mission can be completed. In [7], one of the main research questions is whether it is possible to provide the "blueprint" of a robotic mission without describing the